Cisco Secure Access Control Server アカウンティング要求 バッファオーバーフローの脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070105-CVE-2006-4098 **初公開日 :** 2007-01-05 23:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.0 **回避策 :** Yes **Cisco バグ ID :**	CVE-2006-4098

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Secure Access Control Server for Windows および Cisco Secure Access Control Server ソリューション エンジンは認証される可能にする可能性があるサービス拒否（DoS）状態を引き起こすか、または任意 の コードを実行するために脆弱性リモート攻撃者が含まれています。

CSRadius サービスの不十分な入力の検証による脆弱性存在。 認証されて設計されている悪意のある RADIUS アカウンティング要求を入れることによって、リモート攻撃者 バッファオーバーフローを引き起こすようにこの脆弱性を不正利用する可能性があります。 これは攻撃者がこのサービスをクラッシュするか、またはシステム特権の任意 の コードを実行することを可能にする可能性があります。

Cisco は Security Advisory をリリースし、更新済ソフトウェアをリリースしました。

この脆弱性を不正利用するために、リモート攻撃者は RADIUS 秘密鍵にアクセスできなければなりません。 これは潜在的な攻撃者のプールを下げる必要があります。 不正利用は攻撃者が CSRadius サービスの特権の任意 の コードを実行することを可能にする可能性があります。 これは認証 および 権限 サービスを要請する CSAuth モジュールとデバイス間の通信を提供するのに利用されるサービスです。

攻撃者が CSRadius サービスをクラッシュする場合、すべての RADIUS認証、許可および会計処理は機能し終えます。 ただし、TACACS+ 処理は機能し続けます。

該当製品

修正済みソフトウェア

以下のシスコ製品を稼動するシステムは脆弱です:

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2007-Jan-05

利用規約